Detecting Linear Block Codes in Noise using the GLRT

Arti D. Yardi, Saravanan Vijayakumaran

***Abstract*—In this paper, we consider the problem of distinguishing the noisy codewords of a known binary linear block code from a random bit sequence. We propose to use the generalized likelihood ratio test (GLRT) to solve this problem. We also give a formula to find approximate number of codewords required and compare our results with an existing method.**

I. Introduction

In blind reconstruction of an error correcting code, the aim is to reconstruct the underlying code from noisy version of transmitted codeword sequence without the knowledge of the parameters of the code. For example, this problem arises in cognitive radios or spectrum surveillance applications. This problem was first introduced by Planquette [1] for linear block codes. Valembois proved this problem to be NP-complete [2]. In spite of NP-completeness, Valembois [2], Cluzeau [3] et. al. have suggested various algorithms which make use of information set decoding techniques, such as given by Canteaut et. al. [4]. Sicot, Houcke, Barbier [5], Burel, Gautier [6] have suggested algorithms which make use of Gaussian elimination process.

In this paper, we consider the problem of distinguishing the noisy codewords of a *known* binary linear block code from a random bit sequence. This problem was proposed by Chabot in [7]. The main challenge in this problem is that the codewords which are transmitted are not known to the receiver. The solution proposed in [7] addresses this challenge by computing the inner product of the received bit sequence with codewords in the dual code. The difference in the distributions of the inner product values in the presence and absence of the codewords in the received bit sequence is used to solve the detection problem.

In this paper, we propose a new method which makes use of the generalized likelihood ratio test (GLRT) [8] to solve the code detection problem. The GLRT addresses the issue of the unknown codewords by first estimating them using maximum likelihood decoding and then using the estimates perform a threshold test. The problem formulation is presented in Section II. In Section III we derive the GLRT structure and distribution functions for threshold testing. In Section IV we design a threshold test based on Neyman-Pearson criterion and sequential detection method. We also give a formula to find approximate number of codewords required to achieve a given performance. Performance results of the proposed method and a comparison with an existing technique are presented in Section V followed by some concluding remarks in Section VI.

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Bombay, Mumbai, India 400 076. Email: {arti,sarva}@ee.iitb.ac.in

II. Problem Formulation

We are faced with a binary hypothesis testing problem where the null hypothesis H_0 corresponds to the situation when the observed bit sequence is independent and identically distributed (i.i.d.) bits with each bit equally likely to be zero or one. The alternate hypothesis H_1 corresponds to the situation when the observed bit sequence is the result of passing M unknown codewords of an (n, k) binary linear block code C through a binary symmetric channel (BSC) having crossover probability p. Let the observed bit sequence of length Mn be given by $\mathbf{Y} \in \mathbb{F}_2^{Mn}$. The binary hypothesis testing problem is given by

$$\begin{aligned} H_0 &: \mathbf{Y} \text{ is random bit sequence of length } Mn \\ H_1 &: \mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix} \mathbf{V}_1 & \mathbf{V}_2 & \cdots & \mathbf{V}_M \end{bmatrix} + \mathbf{E} \end{aligned}$$

where $\mathbf{V} \in \mathbb{F}_2^{Mn}$ such that $\mathbf{V}_i \in \mathbb{F}_2^n$ is a codeword in C and $\mathbf{E} \in \mathbb{F}_2^{Mn}$ is the error vector induced by the BSC having crossover probability $p < \frac{1}{2}$. The entries of $\mathbf{E}$ are i.i.d. taking value one with probability p.

Under the null hypothesis H_0, every vector $\mathbf{y} \in \mathbb{F}_2^{Mn}$ is equally likely and hence the probability mass function (pmf) of the observed vector is given by

$$p_0(\mathbf{y}) = \frac{1}{2^{Mn}}. \tag{1}$$

Under the alternate hypothesis H_1, the pmf of the observed vector depends on the unknown codewords transmitted and is given by

$$p_1(\mathbf{y}; \mathbf{V}) \quad = \quad p^{d_H(\mathbf{y},\mathbf{V})}(1-p)^{Mn - d_H(\mathbf{y},\mathbf{V})} \tag{2}$$

where $d_H(\mathbf{y}, \mathbf{V})$ is the Hamming distance between the vectors $\mathbf{y}$ and $\mathbf{V}$.

III. Generalized Likelihood Ratio Test Structure

We propose to use the generalized likelihood ratio test (GLRT) to deal with the problem of the unknown codewords. In this approach, the pmf of the observed vector under the alternate hypothesis will be calculated by substituting the maximum likelihood (ML) estimates of the codewords. The GLRT statistic for the detection problem is given by

$$\Lambda(\mathbf{y}) = \frac{p_1(\mathbf{y}; \hat{\mathbf{V}}_{ML})}{p_0(\mathbf{y})}$$

For BSC, calculation of the ML estimates will involve finding the codewords which are nearest in Hamming distance

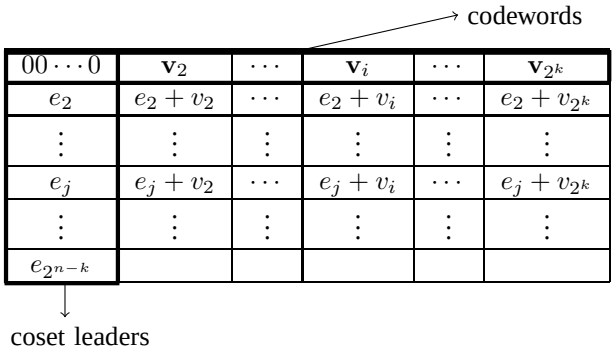

Figure 1. The general structure of a $2^{n-k} \times 2^k$ standard array

to the received vectors [9]. The GLRT decides that H_1 is true if $\Lambda(\mathbf{y})$ exceeds a threshold and decides that H_0 is true otherwise. For a threshold T, this can be represented by

$$\Lambda(\mathbf{y}) \underset{H_0}{\overset{H_1}{\gtrless}} T.$$

Since $p_0(\mathbf{y})$ does not depend on $\mathbf{y}$ and $p_1(\mathbf{y}; \hat{\mathbf{V}}_{ML})$ is a monotonically decreasing function of $d_H(\mathbf{y}; \hat{\mathbf{V}}_{ML})$, the GLRT can be simplified to the form

$$d_H(\mathbf{y}, \hat{\mathbf{V}}_{ML}) \underset{H_1}{\overset{H_0}{\lessgtr}} \tau. \tag{3}$$

To find the optimal threshold τ_{opt} using hypothesis testing methods, we need to characterize the pmf of the GLRT statistic $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML})$ under the two hypotheses. The GLRT statistic can be written as

$$d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) = \sum_{i=1}^{M} d_H(\mathbf{Y}_i, \hat{\mathbf{V}}_i).$$

In fact, the random variables in the sum on the right hand side are i.i.d. since all codewords are independent. If we can obtain the pmf of one of the random variables in the sum, we obtain the pmf of the sum as the M-times discrete convolution of the individual pmf. Without loss of generality we now find the pmf of $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ under both the hypotheses, where $\mathbf{V}_1$ is the first codeword. We consider standard array ML decoding technique to find these pmf's.

A. Standard Array Decoding and Coset Weight Distribution

In standard array, the set of all possible 2^n n-tuple received vectors is partitioned into 2^k disjoint subsets each having 2^{n-k} vectors such that all the vectors in a subset are closest to a particular codeword in $\mathcal{C}$. The general structure of any standard array is shown in Figure 1. More details can be found in [9].

Weight distribution of a code $\mathcal{C}$ is defined as the set of numbers $\{A_j\}$, where A_i is the number codewords of weight i, $0 \leq i \leq n$ [9]. Weight distribution of any row in a standard array and weight distribution of coset leaders is also defined in the same way. All coset leaders and weight distribution of rows corresponding to these coset leaders form the *coset weight distribution* of the code.

Since we assume that the code is known, the coset weight distribution of the code can be found out. We consider this as a pre-calculation phase.

B. GLRT Statistic Distribution under the Null Hypothesis

When the null hypothesis H_0 is true, the received vector $\mathbf{Y}_1$ is equally likely to be any vector in $\mathbb{F}_2^n$. It takes a particular value with probability $\frac{1}{2^n}$.

If the received vector $\mathbf{Y}_1$ falls in the first row of the standard array, it is equal to a codeword in C and the ML estimate is $\hat{\mathbf{V}}_1 = \mathbf{Y}_1$. In this case, $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ is equal to zero. Thus we have

$$\Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = 0; H_0] = \frac{2^k}{2^n} \tag{4}$$

since there are 2^k vectors in the first row of the standard array.

If the received vector $\mathbf{Y}_1$ falls in some row other than the first row of the standard array, it is equal to sum of the coset leader $\mathbf{e}$ of the row and the codeword $\mathbf{v}$ at the top of the column it falls in i.e. $\mathbf{Y}_1 = \mathbf{e} + \mathbf{v}$. Since ML estimate $\hat{\mathbf{V}}_1$ is equal to the codeword at the top of the column $\mathbf{v}$, we have

$$d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = d_H(\mathbf{e} + \mathbf{v}, \mathbf{v}) = w_H(\mathbf{e})$$

where $w_H(\mathbf{e})$ is the Hamming weight of the coset leader $\mathbf{e}$. Let β_j denote the number of coset leaders having weight j. The weight distribution of the coset leaders consists of the numbers $\beta_0, \beta_1, \ldots, \beta_n$. If the received vector falls in any of the β_j rows having coset leaders of weight j, $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ will take the value j. In terms of the coset leader weight distribution we have

$$\Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = j; H_0] = \frac{2^k \beta_j}{2^n}, \tag{5}$$

for $0 \leq j \leq n$, since each of the β_j rows have 2^k vectors in the standard array.

Let $q_0(j) = \Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = j; H_0]$ denote the pmf of $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ under the null hypothesis H_0. Given the pmf of each of the i.i.d random variables in the sum on the right hand side of Equation (4), the pmf of the GLRT statistic $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML})$ can be obtained as

$$Q_0(j) = \underbrace{q_0 * q_0 * \cdots * q_0}_{M \text{ times}}(j), \tag{6}$$

for $0 \leq j \leq Mn$, where $*$ denotes the convolution operator.

C. GLRT Statistic Distribution under the Alternate Hypothesis

Suppose the alternate hypothesis H_1 is true. The received vector $\mathbf{Y}_1$ is equal to the sum of the transmitted codeword $\mathbf{V}_1$ and the error vector $\mathbf{E}_1 \in \mathbb{F}_2^n$ induced by the BSC. As discussed in Section III-B, the statistic $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ is zero if the received vector $\mathbf{Y}_1$ falls in the first row of the standard array. This is possible if and only if the error vector $\mathbf{E}_1$ is equal to a codeword in C. Let A_i be the number of codewords in C having weight i. The probability that $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ is zero is given by

$$\begin{aligned} \Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = 0; H_1] &= \Pr[\mathbf{E}_1 \in C] \\ &= \sum_{i=0}^{n} A_i p^i (1-p)^{n-i} \end{aligned} \tag{7}$$

Note that this probability does not depend on the transmitted codeword $\mathbf{V}_1$.

Let $\mathbf{e}_j$ be the coset leader of the jth row in the standard array. Then the set of all vectors in the jth row of the standard array is given by $\mathbf{e}_j + C$. The probability that the received vector falls in the jth row of the standard array is given by

$$\begin{aligned}\Pr[\mathbf{Y}_1 \in \mathbf{e}_j + C] &= \Pr[\mathbf{V}_1 + \mathbf{E}_1 \in \mathbf{e}_j + C] \\ &= \Pr[\mathbf{E}_1 \in \mathbf{e}_j + C] \\ &= \sum_{i=0}^{n} B_i^{(j)} p^i (1-p)^{n-i} \end{aligned} \quad (8)$$

where $B_i^{(j)}$ is the number of vectors in the jth row with weight i. The sequence $B_0^{(j)}, B_1^{(j)}, \ldots, B_n^{(j)}$ is called the coset weight distribution of the jth row in the standard array. Let $S_l \subset \{1, 2, \ldots, 2^{n-k}\}$ be the set of rows in the standard array whose coset leaders have weight l. Then we have

$$\Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = l; H_1] = \sum_{j \in S_l} \sum_{i=0}^{n} B_i^{(j)} p^i (1-p)^{n-i} \quad (9)$$

for $0 \leq l \leq n$. Note that the above probability does not depend on the transmitted codeword $\mathbf{V}_1$. Since the first row in the standard array is the only row having a zero weight coset leader, we have $S_0 = \{1\}$. We also have $B_i^{(1)} = A_i$ since the coset in the first row of the standard array is the code itself.

Let $q_1(j) = \Pr[d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1) = j; H_1]$ denote the pmf of $d_H(\mathbf{Y}_1, \hat{\mathbf{V}}_1)$ under the alternate hypothesis H_1. From Equation (4), the pmf of the GLRT statistic $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML})$ can be obtained as

$$Q_1(j) = \underbrace{q_1 * q_1 * \cdots * q_1}_{M \text{ times}}(j), \quad (10)$$

for $0 \leq j \leq Mn$, where $*$ denotes the convolution operator.

IV. Threshold Design For The GLRT

Using Equations (4), (5), (7) and (9) we can find pmf of $d_H(\mathbf{Y}, \hat{\mathbf{V}})$ under both the hypotheses. The problem is now to find an optimal threshold τ_{opt} in Equation (3). We apply Neyman-Pearson hypothesis testing method to find τ_{opt}. We also apply sequential detection method.

A. Setting the Neyman-Pearson Threshold

According to the Neyman-Pearson criterion the optimal threshold is given by

$$\tau_{opt} = \underset{\tau}{\operatorname{argmax}}\ P_D(\tau) \text{ under the constraint } P_F(\tau) \leq \alpha$$

where α is the bound on the probability of false alarm. And the optimum decision rule is

1) Decide H_1 is true if $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) < \tau_{opt}$.
2) Decide H_1 is true with probability η if $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) = \tau_{opt}$.
3) Decide H_0 is true if $d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) > \tau_{opt}$.

Here η and τ_{opt} are chosen such that $P_F(\tau_{opt}) = \alpha$. The randomization in the decision rule is necessary because of the discrete nature of the GLRT statistic which may prevent the false alarm probability from being equal to α when a nonrandomized decision rule is used.

The probability of false alarm $P_F(\tau_{opt})$ is given by

$$\begin{aligned} P_F(\tau_{opt}) &= \Pr[d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) < \tau_{opt}; H_0] \\ &\quad + \eta \Pr[d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) = \tau_{opt}; H_0] \\ &= \sum_{j < \tau_{opt}} Q_0(j) + \eta Q_0(\tau_{opt}), \end{aligned} \quad (11)$$

where $Q_0(\tau_{opt}) = 0$ if τ_{opt} is not an integer between 0 and Mn. The probability of detection $P_D(\tau_{opt})$ is given by

$$\begin{aligned} P_D(\tau_{opt}) &= \Pr[d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) < \tau_{opt}; H_1] \\ &\quad + \eta \Pr[d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) = \tau_{opt}; H_1] \\ &= \sum_{j < \tau_{opt}} Q_1(j) + \eta Q_1(\tau_{opt}), \end{aligned} \quad (12)$$

where $Q_1(\tau_{opt}) = 0$ if τ_{opt} is not an integer between 0 and Mn.

To set the optimal threshold, find the largest integer i between 0 and Mn such that $\sum_{j<i} Q_0(j) \leq \alpha$ and set $\tau_{opt} = i$. If $\sum_{j<\tau_{opt}} Q_0(j) = \alpha$, set $\eta = 0$. If $\sum_{j<\tau_{opt}} Q_0(j) < \alpha$, randomization will be required in the decision rule and setting

$$\eta = \frac{\alpha - \sum_{j<\tau_{opt}} Q_0(j)}{Q_0(\tau_{opt})} \quad (13)$$

will result in the false alarm probability being equal to α.

B. Approximate Number of Codewords Required

Define a random variable $X_i^j = d_H(\mathbf{Y}_i, \hat{\mathbf{V}}_i)$, for $i = 1, 2, \ldots, M$ under hypothesis H_j, for $j = 0, 1$. Since the $\mathbf{Y}_i$'s are independent, the X_i^j's are i.i.d. with pmf given by Equations (4), (5), (7) and (9) with mean μ_j and variance σ_j^2.

Define a random variable $\mathbf{X}^j = X_1^j + X_2^j + \ldots + X_M^j$ corresponding to $d_H(\mathbf{Y}, \hat{\mathbf{V}})$. From central limit theorem, the distribution of $\frac{1}{M}\mathbf{X}^j$ can be approximated by a Gaussian distribution with mean μ_j and variance σ_j^2. Let $\Phi(\frac{x-\mu}{\sigma})$ denote cdf of a Gaussian random variable with mean μ and variance σ^2, where $\Phi(x)$ is cdf of standard Gaussian random variable.

Now we know,

$$P_F(\tau_{opt}) = \Pr[\frac{1}{M} d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) < \tau'_{opt}; H_0] = \alpha$$

$$P_D(\tau_{opt}) = \Pr[\frac{1}{M} d_H(\mathbf{Y}, \hat{\mathbf{V}}_{ML}) < \tau'_{opt}; H_1] = \beta$$

where $\tau'_{opt} = \frac{1}{M}\tau_{opt}$.

From central limit theorem we have,

$$\Phi\left(\frac{\tau'_{opt} - \mu_0}{\sigma_0/\sqrt{M}}\right) = \alpha$$

$$\Phi\left(\frac{\tau'_{opt} - \mu_1}{\sigma_1/\sqrt{M}}\right) = \beta$$

Solving above two equations for M we get

$$M = \left(\frac{\sigma_0 \Phi^{-1}(\alpha) - \sigma_1 \Phi^{-1}(\beta)}{\mu_1 - \mu_0}\right)^2 \quad (14)$$

Using Equation (14) the approximate number of codewords required can be found for a given α and β.

C. Sequential Detection Method

Neyman-Pearson method is a fixed sample method i.e. the number of codewords M are fixed. In the sequential detection method, the number of codewords M_s are varied to achieve a specified α and β [10]. Thus the number of samples M_s is now a random variable.

Let us denote the pmf's $q_0(j)$ and $q_1(j)$ given by Equations (4), (5), (7) and (9) by

$$\begin{aligned} q_0(j) &= \begin{bmatrix} r_0 & r_1 & \cdots & r_n \end{bmatrix} \\ q_1(j) &= \begin{bmatrix} s_0 & s_1 & \cdots & s_n \end{bmatrix} \end{aligned}$$

where r_j is $\Pr[d_H(\mathbf{Y}_i, \hat{\mathbf{V}}_i) = j; H_0]$ and similarly for s_j.

Now consider a sequence of $d_H(\mathbf{Y}_i, \hat{\mathbf{V}}_i)$ corresponding to received codeword sequence. Let a random variable D_j indicate the number of times Hamming distance j was observed in this sequence. Thus the vector $\mathbf{D} = (D_0, ..., D_n)$ follows a multinomial distribution with parameters $\begin{bmatrix} r_0 & r_1 & \cdots & r_n \end{bmatrix}$ under hypothesis H_0 and with parameters $\begin{bmatrix} s_0 & s_1 & \cdots & s_n \end{bmatrix}$ under hypothesis H_1.

The likelihood ratio λ_m is given by

$$\lambda_m = \frac{s_0^{d_0} \cdot s_1^{d_1} \cdot \ldots \cdot s_n^{d_n}}{r_0^{d_0} \cdot r_1^{d_1} \cdot \ldots \cdot r_n^{d_n}}$$

According to [10], the decision rule is as follows

if $B < \lambda_m < A$, take additional codewords
if $\lambda_m \geq A$, accept H_1, terminate the process
if $\lambda_m \leq B$, accept H_0, terminate the process

where the boundary points A, B are given by

$$A = \frac{\beta}{\alpha} \text{ and } B = \frac{1-\beta}{1-\alpha}$$

From [8], the expected number of codewords M_s required under hypothesis H_0 and H_1 for sequential detection method are given by

$$\begin{aligned} E\{M_s|H_0\} &\cong \frac{1}{\delta_0}\left\{(1-\alpha)\log\frac{1-\beta}{1-\alpha} + \alpha\log\frac{\beta}{\alpha}\right\} \\ E\{M_s|H_1\} &\cong \frac{1}{\delta_1}\left\{(1-\beta)\log\frac{1-\beta}{1-\alpha} + \beta\log\frac{\beta}{\alpha}\right\} \end{aligned} \quad (15)$$

It can be shown that,

$$\delta_0 = \sum_{i=0}^{n} r_i \log\frac{s_i}{r_i} \text{ and } \delta_1 = \sum_{i=0}^{n} s_i \log\frac{s_i}{r_i}$$

Using Equation (15), the expected number of codewords can be found for a given α and β.

V. Performance Results

A. Performance of GLRT method

In this section, we present the performance of the GLRT based code detection scheme for the $(7, 4)$ Hamming code when Neyman-Pearson method is applied. For $\alpha = 0.05$, the probability of detection $P_D(\tau_{opt})$ for the $(7, 4)$ Hamming code is plotted in Figure 2 as a function of the number of noisy codewords observed M for different values of p. For each value of M, the pmf Q_0 is used to set the threshold τ_{opt} and the randomization parameter η. The probability of detection is obtained using Equation (12).

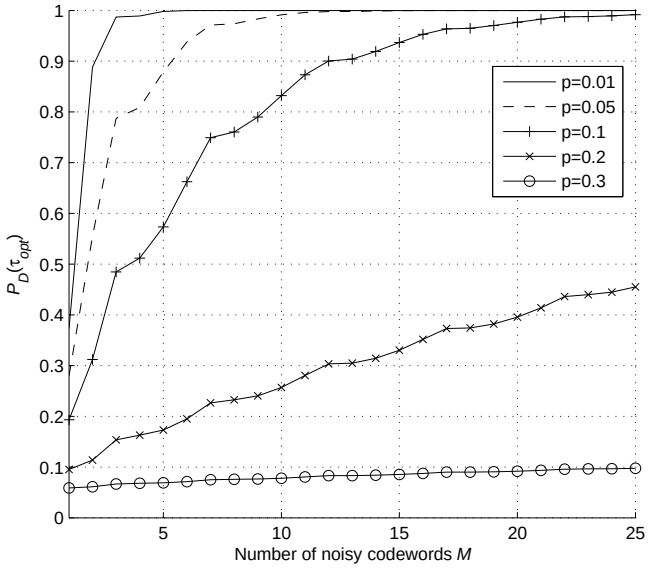

Figure 2. The probability of detection $P_D(\tau_{opt})$ as a function of the number of noisy codewords observed M with $\alpha = 0.05$ for the $(7, 4)$ Hamming code.

For $p = 0.1$, the receiver operating characteristic (ROC) is shown in Figure 3 for different values of M. The ROC is piecewise linear with changes in slope at $\alpha = \sum_{j<i} Q_0(j)$ for $0 \leq i \leq Mn$. For $\alpha \in [\sum_{j<i} Q_0(j), \sum_{j<i+1} Q_0(j))$, the optimal threshold will be chosen to be equal to i and the slope of the ROC is $Q_1(i)$ (see Equation (12)). As one would expect, the shape of the ROC becomes more favorable as the number of noisy codewords observed increases.

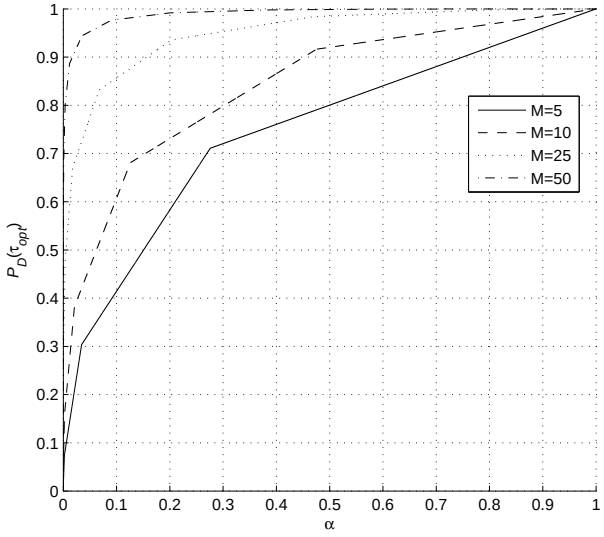

Figure 3. The probability of detection $P_D(\tau_{opt})$ as a function of α for the $(7, 4)$ Hamming code with $p = 0.1$.

B. Comparison of GLRT Method with Chabot's Method

We now compare our method with method proposed by Chabot [7] with respect to number of codewords required to achieve same performance. We use Equation (14) to find number of codewords required by our method. The Table I shows a comparison for various codes for $\alpha = 0.05$, $\beta = 0.997$ and for various values of p. Here, Hamm(n, k) denotes Hamming code and RM(n, k) denotes Reed-Muller code. Coset weight distribution of RM$(64, 22)$ is taken from [11].

Linear Block Code	p	No. of Codewords Required by GLRT method	No. of Codewords Required by Chabot's Method
Hamm(31,26)	0.05	61.50	550.42
	0.07	183.01	2397
Hamm(63,57)	0.05	560.31	16371
	0.07	6.19×10^3	3×10^5
Hamm(127,120)	0.05	1.19×10^5	1.39×10^7
	0.07	3.70×10^7	4.68×10^9
RM(32,16)	0.1	9.25	674.12
	0.15	40.07	5800
RM(64,22)	0.1	49.55	2.44×10^4
	0.15	1.35×10^3	1.75×10^6
BCH(15,7)	0.1	10.39	102.83
	0.15	29.12	322.91
BCH(31,16)	0.1	10.67	674.12
	0.15	46.52	5800

Table I
COMPARISON OF NUMBER OF CODEWORDS REQUIRED BY GLRT METHOD WITH CHABOT'S METHOD

It can be seen from the Table I that the number of codewords required by GLRT method are considerably less than than that of required by Chabot's method. But the challenge in GLRT method is finding the coset weight distribution of the code. Hence the GLRT method is best suited for the codes of moderate length or when coset weight distribution of the code is known.

C. Comparison of Neyman-Pearson and Sequential Detection Method

We now compare the number of codewords required by Neyman-Pearson method denoted by M with that required by sequential detection method denoted by M_s for the same value of p, α and β. Table II shows a comparison for $\alpha = 0.05$, $p = 0.05$ and for various values of β for Hamm$(15, 11)$.

β	No. of Codewords Required by Neyman-Pearson method	No. of Codewords Required by Seq. detection method
0.5787	5	3.0665
0.6953	8	4.2347
0.7738	10	5.1228
0.8980	14	6.7518
0.9218	17	7.1081
0.9561	20	7.6650
0.9962	35	8.4460
0.9973	37	8.4718

Table II
COMPARISON OF NUMBER OF CODEWORDS REQUIRED BY NEYMAN-PEARSON METHOD WITH SEQUENTIAL DETECTION METHOD

In Neyman-Pearson method, we first fix the number of codewords M. Then for a given α we find the decision rule which maximizes the probability of detection β as explained in Section IV-A; while in the sequential detection method, for a given α and β we find the expected number of codewords M_s required using Equation (15). It can be seen that the number of codewords by sequential detection method are less than that of Neyman-Pearson method.

VI. CONCLUSION

In this paper, we have derived a new method for detecting binary linear block codes in noise based on GLRT. The GLRT method involves ML decoding of the received bit sequence and performing a threshold test on the Hamming distance between the ML estimates of the codewords and the received bit sequence. In this work, we choose the threshold according to the Neyman-Pearson criterion and the sequential detection method. We observe that the number of codewords required by our method is considerably less when compared with the existing method. This method is suitable for codes of moderate length or when the coset weight distribution of the code is known.

Note that in this method we have assumed that codewords are perfectly synchronized. The problem of detecting the first bit of the codeword is discussed by Sicot et. al. [12]. One future direction will be to extend this GLRT based method when codewords are not perfectly synchronized.

ACKNOWLEDGEMENTS

The authors would like to thank Prof. Animesh Kumar for useful discussions regarding this problem. The authors would like to acknowledge the support of the Bharti Centre for Communication at IIT Bombay which made this work possible.

REFERENCES

[1] G. Planquette, "Identification de trains binaires codés," *Ph.D. Thesis*, Universite de Rennes I, France, 1996.
[2] A. Valembois, "Detection and recognition of a binary linear code," *Discrete Applied Mathematics*, vol. 111, pp. 199–218, July 2001.
[3] M. Cluzeau, "Reconnaissance d'un schéma de codage," *Ph.D. Thesis*, École polytechnique 2006.
[4] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 367–378, January 1998.
[5] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal Processing*, vol. 89, no. 4, pp. 450–462, April 2009.
[6] G. Burel and R. Gautier, "Blind estimation of encoder and interleaver characteristics in a non cooperative context," in *Proceedings of the IASTED International Conference on Communications, Internet and Information Technology*, Scottsdale, AZ, USA, 2003.
[7] C. Chabot, "Recognition of a code in a noisy environment," in *Proceedings of IEEE ISIT*, June 2007, pp. 2211–2215.
[8] H. V. Poor, *Introduction to Signal Detection and Estimation*, 2nd ed. New York: Springer-Verlag, 1994.
[9] S. Lin and D. Costello, *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004.
[10] A. Wald, *Sequential Analysis*. Wiley and Sons, 1947.
[11] M. Ozeki and K. Waki, "Complete coset weight distributions of second order reed-muller code of length 64," *Journal of Math-for-industry*, vol. 3A, pp. 1–20, 2011.
[12] R. Imad, S. Houcke, and G. Sicot, "Blind frame synchronization for error correcting codes having a sparse parity check matrix," in *IEEE Transactions on Communications*, vol. 57, June 2009, pp. 1574–1577.